虚拟网络技术在计算机网络安全中的应用

宋凌梅
（中共玛纳斯县委员会网络安全和信息化委员会办公室，新疆 昌吉州　832200）

摘　要：自21世纪以来，我国计算机及互联网普及程度不断提高，计算机及互联网技术已经渗透至公众生产、生活的各个环节中，成为社会生活与生产必备的工具之一。“科学技术是一把双刃剑”，计算机网络在为公众创设多元化、交互式信息流通空间的同时也带来了诸多问题，其中计算机网络安全问题尤为突出，如因个人操作不当或安全意识薄弱引发的信息泄露问题、因安全防范措施不到位引发的黑客攻击问题等都在威胁着公众的信息与财产安全。为此，亟须应用先进的虚拟网络技术提升计算机网络的安全性，为计算机网络用户提供优质、安全的信息传播、存储、内容等服务。文章从虚拟网络技术的特点及类型入手，以云计算、密钥、数据加密等虚拟网络技术为核心设计计算机网络安全系统，旨在为计算机网络安全管理与防护提供思路。

关键词：虚拟网络技术；特点类型；计算机；网络安全；系统设计　　**中图分类号：**TP393　　**文献标识码：**A
文章编号：1671-0134（2021）02-105-03　　**DOI：**10.19483/j.cnki.11-4653/n.2021.02.031
本文著录格式：宋凌梅．虚拟网络技术在计算机网络安全中的应用[J]. 中国传媒科技，2021（02）：105-107.

导语

虚拟网络技术开辟了网络服务的新空间，使计算机网络用户能够随时随地浏览、应用海量的网络资源，并能够突破地域、实践的限制在相应的终端完成数据存储、扩展等一系列操作。虚拟网络技术应用背景下，计算机网络安全问题也呈现出新形势与新特征，网络病毒、黑客攻击等利用计算机网络安全漏洞窃取、篡改、非法使用个人计算机上的数据，使用户面临着信息安全与财产安全的威胁。传统的计算机网络安全管理与防范方式将数据存储在相应的服务器中，用户需要通过区域网络及服务器才能获取信息，虽然能够在一定程度上保护了用户数据的安全性，但从存储服务器中提取数据会造成数据的时间差，降低数据的精准性与及时性。基于虚拟网络技术的计算机网络安全管理系统具有伸缩性强、连续可用等优势，将分布的数据整合为集中化管理的数据中心，既可以实现服务器与存储数据的有效分离，又能够最大程度保证用户数据的安全性。下文将简要阐释虚拟网络技术的特点与类型，重点分析虚拟网络技术在计算机网络安全中的应用策略。

1 虚拟网络技术概述

1.1　虚拟网络技术的特点

虚拟网络是指，计算机网络中包含一部分虚拟链接，换言之，即为两个计算设备之间不通过网线等进行物理链接，而是以网络虚拟化的方式为两个计算设备传输数据。虚拟网络技术是指通过网络虚拟化，将公共的网络区域转化为特定的网络使用区域，构建私有网络，继而通过数据加密、身份认证等方式保护计算机网络安全的技术。[1]

虚拟网络技术是网络技术中重要的组成部分，其应用于计算机网络中，不仅可以提升计算机网络的安全性，而且有助于创设更为稳定、功能更加多元的计算机网络环境。与此同时，虚拟网络技术可以有效解决计算机网络安全问题，如虚拟网络技术可以在很大程度上避免数据传输的失真、防范病毒、黑客等攻击计算机网络系统、降低数据丢失、损坏、被窃取事件的发生概率等。除此之外，虚拟网络技术的应用可以为用户提供更为优质的计算机网络存储、传输、保存、扩展等服务，为用户的生活及工作提供便利。[2]

虚拟网络技术具有结构简单、应用成本较低等特点。[3]其一，虚拟网络技术的应用可以改善原有的计算机网络结构，剔除原本计算机网络系统内冗余的内容，继而有效提升计算机网络安全管理与维护的质效；其二，虚拟网络技术可减少设备间的物理链接，继而降低计算机网络建设的成本。

1.2　虚拟网络技术的类型

虚拟网络技术通常包括加密技术、身份认证技术、密钥加密技术三大类型。

加密技术是计算机网络安全中常用的虚拟网络技术，其原理为基于一定的算法、数据语言操作方式等将公共网络中的数据转化为加密形式，当经加密的数据传输至用户计算机网络系统后，再经过解密转化为普通的数据。[4]此种虚拟网络技术应用较为广泛，能够在很大程度上保证数据传输的安全性与保密性，并且可以在很大程度上避免数据传输失真，因此具有较高的使用价值。

身份认证技术的原理为：用户在计算机网络内部的信息库中开设专门、独立的账户，并且为该账户设置用户名、安全性较高的密码。用户通过登录该专门账户上传其初始信息，以此作为今后数据操作的动态指令。在用户传输数据的过程中，设备之间除了进行数据转化外，还会实时对比内部及初始数据，时时刻刻认证账户使用者的身份，以此来保证数据传输的安全性。[5]

密钥加密技术一般包括私用密钥及公共密钥两种类型。在私用密钥加密机制中，数据采用发送方以及接收方保存的私有密钥进行加密，该技术以发送方与接收方

已经以人工方式交换了密钥，并且不会威胁网络安全性为基础。公共密钥加密机制中，每一用户会有两个密钥，一个由用户自己保存，即私钥，另一个则放置在公共网络区域，当信息发送者想要向用户传递信息时，便使用公开的密钥对其想发送的信息进行加密处理，用户收到信息后则使用私钥对信息进行解密。[6]

2. 虚拟网络技术在计算机网络安全中的应用

在高度信息化时代，计算机网络中信息传播的密度及速度达到的前所未有的高度，如何对海量数据进行处理、如何保证数据转化、传输及存储的安全性是计算机网络安全系统构建亟须解决的问题。[7] 云计算作为分布式计算、并行计算、网络存储与虚拟化等计算机技术融合的产物，能够在几秒钟时间内处理数以万计的数据，加之虚拟化技术、动态可扩展、按需部署、灵活性高的特点，已经成为计算机网络安全服务中不可或缺的网络应用理念。文章该部分以云计算环境为背景，借助加密技术、密钥加密技术构建计算机网络安全系统，具体如下：

2.1 基于虚拟网络技术的计算机网络安全系统设计思路

任何一个计算机网络安全系统的设计都需要以用户的需求为核心。云计算环境下，用户对数据的传输、存储、提取、应用等提出了更高的要求，同时也希望系统具备漏洞自动修复、安全风险智能识别等功能，因此也对计算机网络安全性能有更为多元的要求。[8]

云计算并非仅限于一种网络技术，而是一种新型网络应用与服务思维，旨在构建数据互联互通、共建共享的云数据中心。因此，云计算网络环境下计算机网络安全系统的设计除了要正确、灵活、合理地运用云计算技术外，还需要运用云计算的分布、集中处理思维。当前我国大部分计算机网络安全系统依然采用传统的服务器存储数据模式，随着数据传输及存储量的增加、系统功能的拓展、用户需求的多样化，此类系统已经不能全面满足用户的多元化需求，呈现出极大的滞后性与局限性。为此，文章所设计的计算机网络安全系统融合了虚拟网络技术、网络安全技术、计算机技术、数据存储技术，并将数据存储与管理放置在两个进程中，以避免系统模块间相互干扰，影响系统运行的稳定性。同时，利用虚拟网络技术对系统运行数据进行收集、处理与反馈，有效识别潜在的计算机网络安全风险，避免损害用户的信息与财产安全。

2.2 基于虚拟网络技术的计算机网络安全系统设计方案

2.2.1 计算机网络安全系统云架构设计

要想在计算机网络安全系统中实现虚拟网络技术的有效运用，需要为其创造特定的环境及条件，所设计的计算机网络安全系统云架构需要具备两个关键特征：其一，智能化特征。基于虚拟网络技术的计算机网络安全系统需要具备一定的自我治理能力，智能化响应云平台的要求，因此需要在系统中内嵌自动化技术；其二，敏捷性特征。基于虚拟网络技术的计算机网络安全系统在面对变化或需求信号时，需要具备敏捷的反应能力，并且要随着系统需求的变化而快速调整，因此需要在系统中内嵌虚拟化技术。[9]

文章所设计的基于计算机网络技术的计算机网络安全系统云架构包括两个主要模块，一是网络报文处理模块，以软件形式实现网络报文处理，并通过 TCP 重组、iSCSI 协议解析提取系统传输的数据；二是数据加解密模块，以硬件形式实现数据的加解密。为了保证两个模块进程的有效衔接，采用了共享内存方式进行两个进程的数据传输，继而动态化调整处理器的 CPU，例如网络报文处理模块进程执行较慢，则增加其 CPU 分配比例。同时，通过 MiCA 加解密引擎实现安全系统组网。

2.2.2 计算机网络安全系统总体功能设计

文章所设计的计算机网络安全系统为透明加解密网关式，可能在同一时间内会有海量数据的传输与存储，因此需要尽可能保证系统运行的稳定性，并在最大程度上避免数据的损坏、丢失。最为常用的降低系模块间耦合性、提高系统整体稳定性及容灾性的方法为分离控制平面与数据平面。在该种方式下，计算机网络安全系统高度模块化，并且一个系统模块出现故障后不会影响其他系统模块进程的执行。此外，系统硬件平台选用 Tilera Gx36 芯片，由 36 各 CPU 及外设构成，将该 36 个 CPU 分为控制平面 CPU 与数据平面 CPU。

由于不同用户对计算机网络安全系统的需求不同，因此要针对用户需求设计多种系统功能。一是基于虚拟网络技术全面评估计算机网络安全系统的安全性；二是对识别并发现系统中的潜在风险。在此基础上，计算机网络安全系统的总体功能主要包括三个方面：其一，用户登录注册的保存、加密传输、解密处理、加密存储。其二，生成数字证书功能，用户自主选择所需要加密的文件，并按照上述流程进行加密存储。其三，数据操作功能，用户需要提取信息时要对其进行验证，再经过加密传输至客户端。

2.2.3 计算机网络安全系统功能模块设计

结合上文所述云计算环境下基于虚拟网络技术的计算机网络安全系统的云架构及总体功能，现对控制平面与数据平面通信功能设计、网络报文处理模块功能设计、数据加解密模块功能设计进行分析。

其一，控制平面与数据平面通信功能设计。控制平面 CPU 基于 Linux 系统具备的内核态与用户态双向数据传输机制实现数据包的高速转发。数据平面 CPU 运行在 ZOL 核上。两者之间通过共享内存、套接字方式实现通信。数据平面向控制平面反馈系统运行的参数，以使控制平面智能化感知系统运行的状态；控制平面为数据平面提供说初始化数据、配置管理等功能。

其二，网络报文处理模块功能设计。该模块的功能主要包括两个层面：一是从网口接收到的报文中提取系统传输的数据；二是将由数据加解密模块处理过后的数据恢复为原始的报文格式。具体的功能主要为 TCP 流重组、iSCSI 协议解析、数据拆分、报文复元。

其三，数据加解密模块功能设计。由于该计算机网络安全系统在单位时间内数据传输与存储量较大，因此

采用软件形式，基于 3DES 算法对数据进行加解密处理。

文章所选择的网络报文模块与数据加解密模块采用两组进程同步进行，两进程间的通信基于共享内存实现，其中数据结构为链表队列，网络报文模块所生成的新节点将会添加至链表队列的末尾。数据加解密模块从队头提取节点并进行相应的处理。共享内存中链表队列如下图 1 所示。

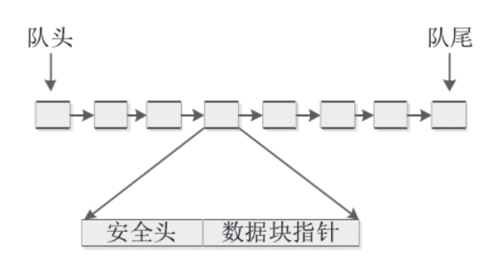


图 1　共享内存中数据链表队列结构示意图

该系统数据加解密模块功能的实现采用 3DES 算法，相对于 DES 算法来说，该算法难以破解，并能通过相应的密钥映射机制增强算法安全性。基于 3DES 算法的加解密原理如下图 2 所示，密钥映射关系如下图 3 所示。

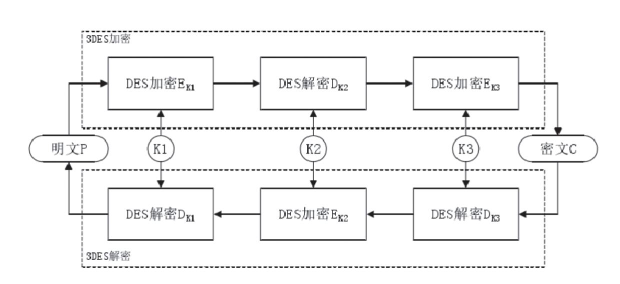


图 2　基于 3DES 算法的数据加解密原理示意图

本地硬盘

映射表

密钥索引	密钥id
密钥索引	密钥id
密钥索引	密钥id
密钥索引	密钥id
密钥索引	密钥id
密钥索引	密钥id
密钥索引	密钥id
密钥索引	密钥id

SQLite数据库

密钥表

密钥id	密钥
密钥id	密钥
密钥id	密钥
密钥id	密钥
密钥id	密钥
密钥id	密钥
密钥id	密钥
密钥id	密钥

图 3　基于 3DES 算法的数据密钥映射关系示意图

结语

计算机网络安全管理与防范是一项系统性、复杂性、长期性与持续性的工程。尤其是在云计算环境下，用户个人计算机网络可以借助网络虚拟化方式灵活介入可类型网络中，如果计算机网络安全防护措施不到位、账户密码保存不及时、个人操作不当等都极有可能成为黑客、病毒以及不法分子的侵入提供可乘之机。因此，亟需采用适宜的虚拟网络技术解决网络安全问题、避免数据传输失真、保障用户隐私、信息及财产安全，继而有效提升计算机网络的安全性。

文章所设计的计算机网络安全系统基于云计算环境，主要原因在于随着科技的发展及计算机与互联网的普及程度进一步提升，用户对于计算机网络系统的功能、计算机网络安全性的需求逐渐提升，其需要在短时间内传输及接收海量的信息，传统的网络应用与处理思维、方式等已经无法满足用户的多元化需求。与此同时，当前云计算已经不再是一种分布计算方式，而是分布计算、网络存储及虚拟化技术融合后的飞跃，具有广阔的发展前景。文章基于云计算环境，借助加解密、密钥加密及数字认证虚拟网络技术设计了能够实现海量数据传输、存储、扩展，并可以保障用户数据安全性的计算机网络安全系统，具有较高的使用价值。

虽然虚拟网络技术与其他网络技术相比优势显著，但鉴于计算机网络安全的特殊性、虚拟网络技术应用不足，虚拟网络技术在计算机网络安全中的应用还局限在较为基础的层面。因此，还需要进一步加大技术的研发力度，将虚拟网络技术应用至计算机网络安全的各个方面，同时要秉承技术性与经济性相统一的原则，继而推动虚拟网络技术的普适性、广泛性发展。媒

参考文献

[1]段翠华 . 计算机网络安全中虚拟网络技术的应用 [J]. 网络安全技术与应用，2021（01）：8-9.

[2] 张存烨 . 简析计算机网络安全中虚拟网络技术的作用与效果 [J]. 电脑编程技巧与维护，2020（12）：144-146.

[3]蓝方力 . 虚拟网络技术在计算机网络安全中的应用 [J]. 网络安全技术与应用，2020（12）：28-29.

[4] 姜大从 . 计算机网络安全中的虚拟网络技术应用与探讨 [J]. 电脑知识与技术，2020，16（30）：30-31.

[5] 童瀛，周宇，姚焕章，梁剑 . 虚拟网络技术在计算机网络安全中的应用价值探析 [J]. 中国新通信，2020，22（20）：85-87.

[6] 杜宇 . 虚拟专用网络技术在计算机网络信息安全中的应用 [J]. 电子技术与软件工程，2020（20）：237-238.

[7] 尹昊乐，郑治华，杨祥一 . 虚拟专用网络技术在计算机网络信息安全中的实践 [J]. 电子技术与软件工程，2020(20)：245-246.

[8]洪小坚 . 虚拟网络技术在计算机网络安全中的应用 [J]. 网络安全技术与应用，2020（10）：41-43.

[9] 王珂 . 大数据时代计算机网络安全防范措施探讨 [J]. 信息与电脑（理论版），2020，32（18）：211-212.

作者简介：宋凌梅（1972-），女，江苏靖江，高级工程师，从事网络安全工作，研究方向：网络安全，网络传输、数据安全等。

（责任编辑：胡杨）